IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method to manage secure communications implemented in a computer-readable medium and to execute on a proxy server, the method, comprising:

establishing, by the proxy server, a secure session on a secure site with an external client that communicates from an insecure site;

detecting, by the proxy server, access attempts during the secure session directed to insecure transactions, the insecure transactions identified as links to a site that is external (external site) to, not controlled by, and not recognized by the secure site, and the access attempts are directed to the insecure transactions having references to resources of the external site; and

transparently managing, by the proxy server, the access attempts by pre-acquiring content from the external site by accessing the links on behalf of the external client to pre-acquire the content and by scanning and inspecting the content within the secure site before determining whether the content should be made available to the external client during the secure session, and at least one access attempt associated with at least one piece of the content that is scanned identifies a true insecure reference by determining that the true insecure reference is a particular reference that has been determined by the method to have had the piece of the content or metadata of the true insecure reference tampered with, and the true insecure reference is entirely removed from the content before the content is supplied to the external client and an event ~~associated with removing the true insecure reference~~ is reported as a custom warning inserted into the content supplied to the external client, the event identifies for the external client within the content that the true insecure reference was removed before being provided to the external client.

2. (Previously Presented) The method of claim 1 wherein the detecting further includes translating any non-secure links into secure links for some of the insecure transactions before

presenting results of the access attempts to the external client.

3-5. (Cancelled).

6. (Previously Presented) The method of claim 1 wherein managing includes at least one or more of:

permitting normally occurring security warnings to present messages to the external client by taking no action;

generating for and displaying to a custom warning message that is presented to the external client;

issuing alerts, notifications, or advisories to a monitoring entity or log; and

determining a number of the links are low-risk to or trusted by the secure site and thereby suppressing normally occurring security warnings from being presented to the external client.

7. (Cancelled).

8. (Currently Amended) A method to manage secure communications implemented in a computer-readable medium and to execute on a proxy server, the method, comprising:

detecting, by the proxy server, insecure transactions occurring during a secure session, the insecure transactions result from actions requested by an external client participating in the secure session;

inspecting, by the proxy server, the insecure transactions in advance of satisfying the actions requested by pre-acquiring content associated with the insecure transactions before making available to the external client, and the insecure transactions are associated with links to an external site located outside a secure site associated with the secure session, and content are pre-acquired from the external site via the links and inspected and scanned on behalf of the external client within the proxy server; and

making, by the proxy server, a determination based on the inspection for taking processing actions including one or more of the following: permitting some of the insecure

transactions to proceed unmodified by performing the actions requested for the external client;

permitting, by the proxy server, some of the insecure transactions to proceed in a modified fashion; and denying some of the insecure transactions by denying the actions requested, and some of the insecure transactions that are denied are identified as references that have a World-Wide Web (WWW) cookie associated with their headers, and ~~wherein~~ these references are entirely removed from the content before the content is supplied to the external client and the references entirely removed are reported as custom warning messages ~~inserted into content supplied~~ to the external client as an event within the content, the event identifies for the external client within the content that the true insecure reference was removed before being provided to the external client.

9. (Cancelled).

10. (Previously Presented) The method of claim 8, wherein the making a determination further includes, permitting some of the insecure transactions to proceed in the modified fashion by changing the reference links from Hypertext Transfer Protocol (HTTP) insecure links to HTTP over Secure Sockets Layer (HTTPS) in order to suppress security warning messages.

11. (Cancelled).

12. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed unmodified by permitting normally occurring security warnings to be presented to the external client before satisfying the external client access attempt to reference the external site.

13. (Previously Presented) The method of claim 8 wherein the making a determination further includes permitting some of the insecure transactions to proceed in a modified fashion by transparently processing the external client access attempt within the proxy server making the external client access attempt appear to be part of the secure session.

14. (Previously Presented) The method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and notifying the external client of a denial.

15. (Previously Presented) The method of claim 8 wherein the making a determination further includes denying the some of the insecure transactions after determining that the external client access attempt is corrupted and logging information about the external client access attempt.

Claims 16-30. (Cancelled).